https://doi.org/10.26552/ pas.Z.2025.1.34

UNIVERSITY OF ŽILINA

DETEKCIA RUŠENIA GNSS SIGNÁLU PROSTREDNÍCTVOM ADS-B PRIJÍMAČOV

Oliver Trnkus
Air Transport Department
University of Žilina
Univerzitná 8215/1
010 26 Žilina

Andrej Novák
Air Transport Department
University of Žilina
Univerzitná 8215/1
010 26 Žilina

Abstract

In this thesis, the detection of GNSS interference by ADS-B receivers and its impact on the accuracy of air navigation is investigated. GNSS systems are important for modern aviation and can be jammed, which threatens the safety of air traffic. ADS-B is a GNSS dependent system which allows monitoring and identification of areas of increased interference. As GNSS jamming events become more frequent, there is an increasing need for reliable approaches to detect jamming and minimise its impact. ADS-B can help to identify unusual deviations in navigation and contribute to improving the safety of air traffic. The survey highlights the need to protect GNSS signals and develop technologies for their detection.

Keywords

GNSS, ADS-B receivers, Interference detection

1. Úvod

Globálne navigačné satelitné systémy (GNSS) dnes patria medzi základné technológie, ktoré sa používajú nielen v bežnom živote, ale najmä v doprave a v letectve. Lietadlá používajú v súčasnosti GNSS hlavne na určenie presnej polohy, GS (ground speed) a ďalších parametrov ako smer vetra, čo je nevyhnutné pre bezpečnú a spoľahlivú navigáciu. V dnešnej dobe bez signálu GNSS by veľa moderných systémov v letectve nefungovalo alebo by sa museli nahradiť menej modernými riešeniami. Práve preto je dôležité, aby bol GNSS signál stabilný a chránený pred rôznymi druhmi rušenia. V posledných rokoch sa čoraz častejšie začali vyskytovať prípady rušenia GNSS signálov. Rušenie môže byť neúmyselné, napríklad ak ho spôsobí iné elektronické zariadenie, ale môže byť aj úmyselné, ako zámerné útoky na systém. Tieto javy môžu spôsobiť vážne problémy, ako chyby údajov o polohe až po úplnú stratu navigačných schopností lietadla. Často nebývajú okamžite viditeľné a prejavujú sa len miernymi odchýlkami v letových trasách.

Tento článok sa zameriava na problematiku rušenia GNSS signálu a na možnosti jeho detekcie prostredníctvom systému ADS-B. Tento systém sa v letectve využíva na monitorovanie a sledovanie lietadiel, pričom určenie polohy závisí od údajov z GNSS, čo z neho robí vhodný nástroj na sledovanie zmien v leteckej prevádzke, ktoré môžu signalizovať rušenie signálu. Zameriava sa tiež na využitie verejne dostupných platforiem ako Flightradar24 a OpenSky Network, ktoré poskytujú údaje o letových trasách a môžu pomôcť identifikovať odchýlky spôsobené rušením GNSS signálu. Tieto platformy umožňujú analyzovať pohyb lietadiel v reálnom čase, čo prispieva k posilneniu bezpečnosti leteckej prevádzky. Na princípe príjmu signálu ADS-B, resp. odpovedí sekundárneho radaru A/C/S z lietadla na frekvencii 1090 MHz, je založených viacero podobných platforiem, no pre účely tohto článku boli vybrané práve tieto dve vzhľadom na ich robustnosť, dostupnosť a celosvetové pokrytie.

2. Metodika a metódy skúmania

Článok vychádza z poznatkov spracovaných z odbornej literatúry, článkov z oblasti GNSS a ADS-B technológií, ako aj z verejne dostupných dátových platforiem ako Flightradar24 a OpenSky Network. Analýza bola zameraná na identifikáciu prípadov rušenia GNSS signálu prostredníctvom sledovania letových dráh v oblastiach so zvýšeným rizikom výskytu anomálií, akými sú náhle odchýlky v trase, výpadky polohy alebo výpadky v prenose dát systému ADS-B.

2.1. GNSS a hlavné zložky

Globálny navigačný satelitný systém, známy pod skratkou GNSS, je technológia umožňujúca na presné určenie polohy a času na ktoromkoľvek miestne na Zemi. Základom tejto technológie sú satelity, ktoré sa nachádzajú na obežnej dráhe Zeme a vysielajú špecifické signály. Tieto signály obsahujú informácie o aktuálnej polohe satelitov, čase vyslania signálu a ďalších parametrov potrebných na výpočet polohy prijímačov na Zemi. Princíp fungovania GNSS spočíva v trilaterácií – teda v určení polohy na základe vzdialeností od niekoľkých satelitov, ktoré sa dajú vypočítať z časového oneskorenia prijatého signálu.

GNSS je postavený na troch hlavných komponentoch. Vesmírny segment zahŕňa satelity, ktoré obiehajú vo výškach 20 000 do 37 000 km nad povrchom Zeme. Tieto satelity vysielajú údaje o svojom stave, polohe a presnom čase. Medzi najznámejšie satelitné navigačné systémy patria GPS, ktoré spravujú USA, GLONASS z Ruska, európsky systém Galileo a čínsky BeiDou. K ním sa pridávajú aj regionálne systémy, ako je japonský QZSS či indický IRNSS, ktoré sa zameriavajú na špecifické oblasti rozšírených služieb pre satelitnú navigáciu, ale aj pre pátranie a záchranu. Ďalšou dôležitou časťou je riadiaci segment, ktorý zahŕňa pozemné stanice zodpovedné za kontrolu a kalibráciu satelitov. Tieto stanice monitorujú dráhy satelitov, aktualizujú ich údaje v databáze almanach a zabezpečujú ich správnu funkciu. Tretím komponentom je užívateľský segment, ktorý

zahŕňa zariadenia, ako sú GPS prijímače v mobilných telefónoch, automobiloch, lodiach, vlakoch, lietadlách alebo špecializované prístroje v oblasti geodézie a kartografie a ďalších odvetví. Vďaka spolupráci všetkých týchto segmentov umožňuje GNSS široké využitie v každodennom živote, od navigácie v autách cez synchronizáciu času v telekomunikačných sieťach až po vedecký výskum a záchranné operácie. Táto technológia je dôležitá pre moderný svet, pričom jej rozvoj pokračuje zavádzaním nových rozšírených satelitných systémov a zlepšovaním presnosti, kontinuity a integrity signálu [1].

2.2. Typy GNSS systémov

V súčasnosti existujú štyri hlavné globálne konštelácie a dve regionálne, ktoré tvoria základ GNSS.

Globálny polohový systém (GPS), spravovaný Spojenými štátmi americkými, je prvým a najstarším systémom GNSS na svete. Jeho činnosť začala v roku 1978, pričom plnú globálnu dostupnosť dosiahol v roku 1994. GPS pozostáva z 31 aktívnych satelitov na obežnej dráhe, ktoré zabezpečuje a riadi americké letectvo. Tento systém poskytuje vysokú presnosť a je jedným z najpoužívanejších na svete.

GLONASS, systém prevádzkovaný Ruskom bol, vyvinutý ako odpoveď na GPS. Prvé testovacie satelity boli vypustené v roku 1982, pričom funkčnosť bola dosiahnutá v roku 1993 so sústavou 12 satelitov. V súčasnosti GLONASS zahŕňa 26 satelitov a jeho prevádzku zabezpečujú ruské letecké obranné sily.

Galileo, európsky navigačný systém, je výsledkom spolupráce Európskej vesmírnej agentúry (ESA) a Agentúry Európskej únie pre vesmírny program (EUSPA). Galileo začal poskytovať služby v roku 2016 a v súčasnosti disponuje 24 aktívnymi satelitmi a dvomi základňami na Zemi. Je to systém zameraný na civilné využitie s vysokou presnosťou.

Navigačný satelitný systém BeiDou (BDS), vyvinutý Čínou, začal ako regionálny systém s obmedzeným pokrytím v roku 2000. Postupom času sa rozšíril na globálny systém, ktorý od roku 2018 poskytuje celosvetové služby. Čína vypustila celkovo 55 satelitov v rámci rôznych generácií systému BDS, pričom v prevádzke je momentálne 35 z nich.

Indický regionálny navigačný satelitný systém (IRNSS), známy aj ako NavIC, je navigačný systém Indie. Jeho konštelácia, pozostávajúca zo siedmich satelitov, začala fungovať v roku 2018. NavIC pokrýva celú Indiu a susedné regióny, pričom ponúka dve úrovne služieb: štandardné pre civilné využitie a šifrované pre autorizovaných používateľov.

Quasi-Zenith satelitný systém (QZSS), ktorý prevádzkuje Japonsko, je regionálny systém určený pre ázijsko-oceánsky región. Jeho konštelácia zahŕňa štyri satelity a systém je funkčný od novembra 2018 [2].

2.3. Čo je ADS-B

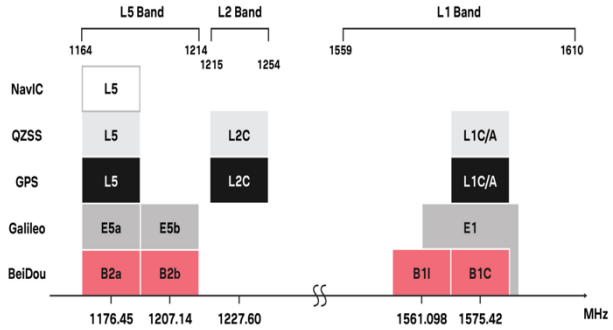
ADS-B, teda Automatic Dependent Surveillance-Broadcast, predstavuje významný technologický pokrok v monitorovaní vzdušného priestoru. Táto technológia využíva transpondér Trig, ktorý je často integrovaný s GPS, na poskytovanie vysoko presných údajov o polohe. Informácie sú prenášané do pozemných riadiacich centier, ako aj priamo k iným lietadlám. Tento typ vysielania sa označuje ako ADS-B Out. V porovnaní s tradičnými radarovými systémami ponúka ADS-B výrazne lepší dosah a presnosť. Vďaka tomu môžu riadiaci letovej prevádzky bezpečne znižovať minimálne rozostupy medzi lietadlami vybavenými ADS-B, čo je dôležité pre efektívne riadenie preťaženého vzdušného priestoru [3]. ADS-B pracuje na princípe vysielania údajov o polohe, rýchlosti a ďalších dôležitých parametroch lietadla, ktoré sú získavané zo systému GNSS. Pozemné stanice, ktoré tieto údaje prijímajú a spracúvajú, sú podstatne lacnejšie ako klasické radary. Tieto stanice slúžia na poskytovanie dát pre situačné displeje, ktoré využívajú riadiaci letovej prevádzky. ADS-B sa stal obzvlášť užitočným v oblastiach bez radarového pokrytia, kde ho niektoré štáty zaviedli na zlepšenie riadenia prevádzky. Tento systém umožnil znížiť rozostupy medzi lietadlami z pôvodných 148,1 km na 9,2 km, čo viedlo k zvýšeniu kapacity vzdušného priestoru. Okrem toho prispel k zníženiu spotreby paliva a emisií, čím sa zlepšila ekologická udržateľnosť leteckej dopravy [4].

2.4. Definícia rušenia GNSS signálov a ako k tomu dochádza

Globálny navigačný satelitný systém (GNSS) pomáha zlepšiť výkonnosť navigácie a podporuje dohľad riadenia letovej prevádzky. GNSS vie dosiahnuť všetky výhody len vtedy, ak sú signály GNSS primerane chránené pred elektromagnetickým rušením, ktoré by mohlo spôsobiť stratu alebo zhoršiť služby GNSS. Zdrojmi rušenia GNSS môžu byť systémy ktoré pracujú v rovnakých frekvenčných pásmach ako GNSS ale aj systémy ktoré sú pracujúce mimo týchto pásiem. To naznačuje že rušenie môže byť úmyselné ale aj neúmyselné [5]. Rušenie GNSS zahŕňa akékoľvek druhy rušenia, ktoré môžu narušiť normálne fungovanie navigačných systémov založených na GNSS. Rozdeľujú sa na dve hlavné kategórie a to je jamming (rušenie signálu) a spoofing (falošné signály) [6]. GNSS signály sú príliš citlivé na rádiofrekvenčné rušenia. Spoločnosť Septentrio sa už 15 rokov zaoberá riešením tohto problému a zdokonaľuje jedinečné systémy na zmiernenie rušenia, adaptívneho filtrovania, vypínania impulzov a jedinečné zmierňovanie rušenia v širokom pásme [7]. Pre rušenie GNSS sa vytvárajú signály, ktoré sú dostatočné silné na to, aby prekonávali vysielanie zo satelitov GNSS. Hoci signály GNSS sa vysielajú z obežnej dráhy sú zvyčajne z výšky viac ako 6 km nad povrchom Zeme, potrebujú prekonať veľké vzdialenosti pokým sa dostanú k pozemným staniciam alebo prijímačom. To spôsobuje že vytvára signál s nízkym výkonom a robí ich čoraz viac zraniteľnými voči rádiovému rušeniu a proti útoku carry-off (bežný útok typu spoofing).

Aj keď satelitné signály môžu byť rušené neúmyselne, často ide o zámerný cieľ a čoraz viac jednotlivcov a subjektov používa stratégie na rušenie GNSS signálov, zvyčajne s cieľom zabrániť sledovanie zariadení ako aj vozidiel, lodí alebo lietadiel. GNSS satelity sa spoliehajú na tri hlavné pásma rádiových frekvencií a to L1, L2 a L5 ktoré sú zobrazené na obrázku 1. Kým väčšina starších satelitov využíva pásma L1 a L2, novšie systémy sú navrhnuté tak, aby pracovali v pásme L5, ktoré ponúka vyššiu presnosť a spoľahlivosť. Tieto systémy však používajú veľmi slabé rádiové signály, ktoré sú náchylné na rušenie. Takéto rušenie môže vážne ovplyvniť presnosť údajov o polohe, čase či rýchlosti, čo vedie k problémom s navigáciou.

Zdroj: https://content.u-



blox.com/sites/default/files/documents/GPS-signals-migration-wp.pdf

Obrázok 1: Frekvencie a rozloženie kanálov v pásme L

Keďže veľká časť infraštruktúry je závislá od GNSS systémov, ich rušenie môže spôsobiť nielen technologické výpadky, ale aj výrazné ekonomické škody. Z tohto dôvodu je ochrana GNSS signálov kriticky dôležitá o čom svedčí aj právna úprava zameraná na monitorovanie a detekciu rušenia signálov [8].

2.4.1. Jamming (rušenie signálu)

Neúmyselné rušenie často spôsobujú rôzne elektronické zariadenia. Problémy môžu nastať v dôsledku signálov v blízkosti spektra GNSS alebo priamo v ňom. Napríklad zariadenia USB 3.0 či niektoré LIDAR senzory môžu vytvárať rušenie v pásme GPS L1 (1575,42 MHz $\pm$ 10MHz), čo vedie k nepresnostiam v určovaní polohy, ak nie je zabezpečené dostatočné tienenie. Zámerné rušenie je známe ako jamming, spočíva vo vysielaní silných rádiových signálov, ktoré potlačiť slabšie GNSS signály, čím sa zabráni správnej funkcií prijímačov v danej oblasti. Je potrebné zdôrazniť, že zámerné rušenie nie je len otázkou vojenských konfliktov ale často ho spôsobujú lacné a nelegálne GPS rušičky, používané na znemožnenie sledovania polohy áut alebo nákladných vozidiel. Rušenie GNSS predstavuje úmyselné blokovanie GNSS signálov pomocou zariadení, ako sú softvérovo definované rádiové vysielače, ktoré vysielajú signály vo frekvenčných pásmach GNSS. V minulosti bolo rušenie bežné v určitých oblastiach, napríklad na hranici medzi Severnou a Južnou Kóreou. Takéto rušenie však nie je obmedzené len na konfliktné zóny, pretože zariadenia na ochranu súkromia sú voľne dostupné. Tie často bránia monitorovaniu vodičov nákladných vozidiel. Hoci rušenie môže byť problematické, nie je také sofistikované ani presné ako spoofing [10].

2.4.2. Spoofing (falošné signály)

Spoofing predstavuje zámerné vysielanie falošných GNSS signálov s cieľom oklamať prijímač, ktorý následne hlási nesprávnu polohu alebo čas. Tento typ útoku je vždy úmyselný a vykonáva sa tak, že rušenie preťaží prijímač, po čom nasleduje vysielanie falošného satelitného signálu. Spoofer využíva rovnakú štruktúru a frekvenciu ako GNSS signály, pričom manipuluje ich výkonnosť tak, aby prijímač preferoval vysielaný signál. Proces spoofingu GNSS signálov je znázornený na obrázku 4 [9]. V leteckých aplikáciách môže spoofing cielenie útočiť na konkrétne lietadlá. Útočník, ktorý pozná ich polohu, môže vysielať falošné signály a ovplyvniť ich navigáciu. Tento druh útoku vyžaduje značné zdroje a sofistikované vybavenie, často spájané s aktérmi, ako sú štátne organizácie alebo teroristické skupiny. Na ochranu pred spoofingom sa využívajú kódované signály GNSS a kombinácia GNSS s inerciálnymi navigačnými systémami (INS), ktoré nie sú náchylné na manipuláciu [10].

3. Zdroje ADS-B dát pre analýzu

Flightradar24 vznikol pôvodne ako hobby projekt ešte v roku 2006, keď sa dvaja leteckí nadšenci zo Švédska rozhodli vybudovať vlastnú sieť ADS-B prijímačov v severnej a strednej Európe. V roku 2009 sprístupnili túto sieť aj ostatným používateľom, ktorí mohli svoje údaje zo svojich prijímačov posielať do systému. Postupne sa tak podarilo pokryť mnohé časti sveta, no snaha o zabezpečenie celosvetového pokrytia ADS-B stále pokračuje [11]. V súčasnosti predstavuje globálnu platformu na monitorovanie letovej prevádzky, ktorá poskytuje aktuálne údaje o pohybe lietadiel po celom svete. Systém využíva kombináciu rôznych zdrojov dát, predovšetkým ADS-B a MLAT, doplnených o satelitné a radarové informácie. Tieto lokalizačné údaje sú následne spracované a obohatené o informácie a o letovom poriadku a taktiež o stave letu, čím vzniká komplexný prehľad o leteckej doprave v reálnom čase [12].

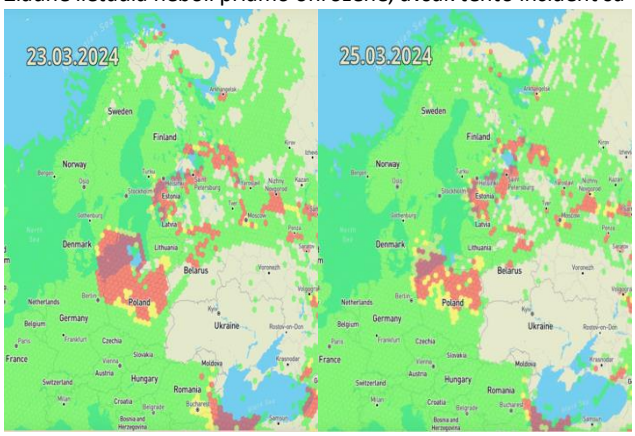
OpenSky Network je nezisková organizácia so sídlom vo Švajčiarsku, ktorá sa zameriava na zlepšenie bezpečnosti, spoľahlivosti a efektívnosti riadenia vzdušného priestoru. Jej základom je rozsiahla sieť prijímačov spravovaných dobrovoľníkmi, priemyselnými partnermi a akademickými či vládnymi inštitúciami. Všetky zhromaždené dáta sú archivované v rozsiahlej historickej databáze, ktorá poskytuje výskumníkom prístup k údajom pre analýzu a optimalizáciu riadenia letovej prevádzky [13].

Táto platforma bola spustená v roku 2013 a odvtedy zabezpečuje systematický zber údajov o letovej prevádzke prostredníctvom technológií ako ADS-B, Mód-S, TCAS, a FLARM. Na rozdiel od iných platforiem poskytuje OpenSky Network úplné, nefiltrované a surové dáta, ktoré sú dostupné predovšetkým akademickej a výskumnej sfére. V súčasnosti spravuje viac než 5 000 prijímačov po celom svete a disponuje databázou obsahujúcou vyše 30 biliónov zachytených správ. Týmto spôsobom predstavuje jeden z najrozsiahlejších zdrojov dát o letovej prevádzke, čo umožňuje podrobnú analýzu a výskum GNSS interferencií či vývoj inovatívnych riešení pre zvýšenie bezpečnosti v letectve [14].

3.1. Neočakávané zmeny trasy a výpadky signálu

V roku 2024 koncom marca, došlo v severnej Európe k masívnemu rušeniu GPS signálov, ktoré ovplyvnilo viac ako 1600 lietadiel. Podľa všetkých indícií pochádza zdroj tohto rušenia z Kaliningradu v Rusku. Lietadlá lietajúce nad Poľskom, Švédskom a ďalšími štátmi v Pobaltí zaznamenali výrazne výpadky GPS signálov. Tento incident je považovaný za najrozsiahlejší prípad rušenia GPS v tejto oblasti, ktorý bol kedy zaznamenaný. Podľa gpsjam.org a Flightradar24 zasiahlo rušenie najmenej 1600 lietadiel, pričom najväčšie výpadky sa vyskytli medzi 23. a 25. marcom 2024 viď na obrázku 2.

Žiadne lietadlá neboli priamo ohrozené, avšak tento incident sa



Obrázok 2: Rušenie signálu GPS v údajoch 23.3.2024 a 25.3.2024

považuje za znepokojujúci prejav kybernetickej vojny. Mnohé zdroje za príčinu tohto rušenia označujú Ruskú federáciu, pričom podozrenia vedú k oblasti Kaliningradu, ruskému územiu ležiacemu medzi Poľskom a Litvou. Nie je vylúčené, že ide o náhodu no od roku 2018 do roku 2021 Eurocontrol zaznamenal dramatický nárast porúch navigačných systémov, konkrétne 20-násobný vzostup prípadov spôsobených rádiovým rušením. Odhady medzinárodnej organizácie pre bezpečnosť leteckej dopravy naznačujú, že tieto výpadky sú prevažne dôsledkom používania rušičiek v oblastiach aktívnych alebo potenciálnych vojenských konfliktov. Rušičky môžu byť nasadené s cieľom zabrániť použitiu raketových a iných vojenských alebo výskumných prostriedkov. Medzi známe oblasti s nespoľahlivým GPS signálom patrí okrem Kaliningradu aj Cyprus, Turecko, Sýria a Izrael. Okrem zjavného rušenia signálov sa piloti niekedy stretávajú aj s falošnými GPS signálmi. Tento trend vyvoláva obavy, že narušenie navigačných systémov je súčasťou širšej kybernetickej a vojenskej taktiky [15].

4. Výsledky

V rámci článku boli predstavené možnosti využitia verejne dostupných platforiem, ako sú Flightradar24 a OpenSky Network, ktoré poskytujú dáta zo systému ADS-B v reálnom čase. Hoci nebola vykonaná vlastná analýza dát, na základe štúdia odborných zdrojov a prípadových štúdií bolo poukázané na to, že tieto platformy môžu byť užitočné pri sledovaní možných výpadkov alebo odchýlok v polohe lietadiel.

Pozorované anomálie v iných štúdiách často súviseli s náhlymi zmenami letovej trasy, výpadkami signálu alebo nestabilným správaním ADS-B údajov, najmä v oblastiach so známym výskytom GNSS rušenia, ako je východná Európa alebo Blízky východ. Takéto prípady naznačujú, že ADS-B môže slúžiť ako indikátor narušenia navigačného signálu.

5. Záver

Článok sa venoval problematike rušenia GNSS signálu a možnostiam, ako môže systém ADS-B prispieť k jeho detekcii. V teoretickej časti boli predstavené princípy fungovania GNSS systémov, ich zraniteľnosti a dôvody, prečo je ochrana týchto signálov dôležitá najmä v letectve. Pozornosť bola zameraná aj na ADS-B systém, ktorý je na GNSS priamo naviazaný a vďaka tomu dokáže indikovať možné problémy s navigáciou. Opísané boli aj prípady rušenia GNSS vo svete a oblasti, kde sa takéto rušenie vyskytuje najčastejšie, ako aj možnosti využitia verejných platforiem Flightradar24 a OpenSky Network pri sledovaní potenciálnych výpadkov signálu.

Z analýzy poznatkov vyplýva, že rušenie GNSS signálu má rastúci trend a v prostredí letectva predstavuje významné riziko. Spoľahlivosť satelitnej navigácie je pre moderné letectvo kľúčová a jej výpadky môžu ovplyvniť bezpečnosť a plynulosť prevádzky. Aj keď ADS-B nebol navrhnutý ako nástroj na detekciu rušenia, jeho prepojenie s GNSS z neho robí účinný indikátor možných anomálií.

V praxi možno pozorovať situácie, v ktorých sa na základe ADS-B dát vyskytujú náhle odchýlky v polohe či výpadky signálu, čo môže signalizovať rušenie alebo jeho zneužitie. Sledovanie týchto údajov môže významne prispieť k včasnej identifikácii rizikových oblastí. Ako perspektívne riešenie sa javí využívanie dostupných platforiem, ktoré by mohli automaticky vyhodnocovať dáta z viacerých zdrojov a spoľahlivo identifikovať podozrivé javy. Rovnako je dôležité vytvárať legislatívne a prevádzkové rámce na efektívne zdieľanie informácií medzi štátmi, leteckými spoločnosťami a poskytovateľmi služieb, ako aj zvyšovať povedomie o problematike rušenia GNSS medzi pilotmi, riadiacimi letovej prevádzky a technickým personálom.

Referencie

[1] HEXAGON. What are Global Navigation Satellite Systems? novatel.com [online]. Cit z : https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss [cit 2 marec 2025 a].

[2] WINDWARD, 2024. Global Navigation Satellite System (GNSS). Windward [online]. 2024. Cit z : https://windward.ai/glossary/gnss-global-navigation-satellite-systems/ [cit 2 marec 2025].

[3] TRIG, 2014. Introduction to ADS-B. Trig Avionics [online]. 23 september 2014. Cit z : https://trig-avionics.com/knowledge-bank/ads-b/introduction-to-ads-b/ [cit 2 marec 2025].

[4] ICAO, 2012. Global Navogation Satellite System (GNSS) Manual [online]. ICAO. Cit z : https://www.icao.int/meetings/anconf12/documents/doc.%209849.pdf [cit 2 marec 2025].

[5] SKYBRARY. Interference to GNSS Signals. SKYbrary [online]. Cit

z : https://skybrary.aero/articles/interference-gnss-signals [cit 2 marec 2025].

[6] GPSPATRON, 2023. GNSS Interference Monitoring and Classification for Critical Infrastructure Safety | GPSPATRON.com. GPSPATRON [online]. 31 január 2023. Cit z : https://gpspatron.com/gnss-interference-monitoring-and-classification-for-critical-infrastructure-safety/ [cit 2 marec 2025].

[7] SEPTENTRIO, 2020. GNSS Interference [online]. ESA-Pierre Carril. Cit z : https://www.ion.org/gnss/upload/files/2157_Septentrio_GNSS_Interference_A5_LR.pdf [cit 2 marec 2025].

[8] GNSS JAMMING. GNSS Jamming. GNSS Jamming [online]. Cit z : https://www.gnssjamming.com/gnss-jamming [cit 2 marec 2025].

[9] SBS SYSTEMS, 2024. SBG Systems response to GNSS Jamming and Spoofing. Linkedin [online]. 15 január 2024. Cit z : https://www.linkedin.com/pulse/sbg-systems-response-gnss-jamming-spoofing-sbgsystems-yso9e [cit 3 marec 2025].

[10] HEXAGON. Spoofing. Hexagon [online]. Cit z : https://novatel.com/an-introduction-to-gnss/gnss-threats/spoofing [cit 3 marec 2025 b].

[11] ECA PILOTING SAFETY, 2024. Manipulated GNSS Signals: implications for pilots. ECA Piloting Safety [online]. 29 apríl 2024. Cit z : https://www.eurocockpit.eu/news/manipulated-gnss-signals-implications-pilots [cit 3 marec 2025].

[12] LOMAS, Chris, 2025. How does Flightradar24 track aircraft? | Flightradar24 Blog. Flightradar24 [online]. 30 január 2025. Cit z : https://www.flightradar24.com/blog/inside-flightradar24/how-does-fr24-track-aircraft/ [cit 3 marec 2025].

[13] UNIVERSITY OF TORONTO. OpenSky Network databases. University of Toronto Libraries [online]. Cit z : https://mdl.library.utoronto.ca/collections/numeric-data/statistics/opensky-network-databases [cit 3 marec 2025].

[14] ELTON, Ahmed, 2023. Open Air Traffic data - OpenSky Network. *kaggle* [online]. 2023. Cit z : https://www.kaggle.com/datasets/ahmedeltom/open-air-traffic-data-opensky-netwrok [cit 12 apríl 2025].

[15] FLIGHTRADAR24. How flight tracking works. *Flightradar24* [online]. Cit z : https://www.flightradar24.com/how-it-works [cit 12 apríl 2025 b].

[16] KASÍK, Pavel, 2024. Masivní útok na GPS zasáhl 1600 letadel. Stopy vedou do ruského Kaliningradu - Seznam Zprávy. *Seznam Zprávy* [online]. 9 apríl 2024. Cit z : https://www.seznamzpravy.cz/clanek/zahranicni-masivni-utok-na-gps-zasahl-1600-letadel-stopy-vedou-do-ruskeho-kaliningradu-249404 [cit 3 marec 2025].